HE Insight

Risk Briefing – Beyond Higher Education

February 2018

Late in 2017, the Institutes of Internal Audit across Europe (UK and Ireland, France, Italy, Netherlands, Spain and Switzerland) pooled their resources to identify common themes or hot topics that could help to focus the attention of internal audit in its efforts to mitigate risk and add value in organisations. The exercise included a wide range of sectors – construction / infrastructure, financial services, IT, manufacturing, public sector, retail / consumer, telecoms and utilities / energy.

We have captured the main risks in the table below with the intention of aiding the development or update to internal audit plans over the coming twelve months. The risks are not in any order.

Risk Theme	Comment
GDPR and the data protection challenge	Along with other sectors, ensuring compliance with the GDPR by the deadline in May is focussing both management time and input from auditors. Perspective wise, it is estimated that under GDPR the £400K fine issued by the UK's Information Commissioner's Office to broadband group TalkTalk for its publicised data security failings two years ago would have potentially risen to £59m. A few thoughts: • consideration should be given to further internal audits beyond the May deadline – these could either assess on going progress and compliance and / or, in a similar way to our approach on cyber related reviews, concentrate on specific elements of the requirements where institutions have concerns or feel there may be more appropriate approaches; • 'tone from the top' is a phrase often used but what does it mean in the context of GDPR compliance? What happens if staff don't undertake the necessary training – are there any consequences, has the Board got members with the necessary background and skills to assess the adequacy of progress within the institution and, if necessary to challenge the executive; • are institutions thinking more broadly about data – stepping back and considering creation, protection and management?
Cyber security: a path to maturity	The importance of gaining assurance about cyber related risks continues. The Wannacry and later Petya, global attacks, mean it's no surprise that this risk appears across the sectors. From all surveyed, there is increased focus on IT and cyber related risks. Potential focus and thoughts as we develop our annual programmes include: • the continuing trend towards the Cloud; increased data dependency, and digital led business models mean that audit programmes need to develop in tandem and cover, for example, exposure to external cyber criminals and hackers as well as malicious employees and careless workers who fail to follow procedures (within and beyond the institution); • controls and technical defences such as firewalls need to be complemented by an embedded cyber culture that manifests itself in staff behaviour and is developed through

Risk Theme	Comment
	companywide training and awareness programmes. Is training seen as a one off or part of an on-going engagement which develops in line with the changing risks? • there can be a focus on digital disruption and innovation but are actions adequate for the legacy systems? • aligned to comments above on GDPR, is the governance surrounding approaches to managing the risks fit for purpose? Does the Audit Committee have the expertise to support and challenge / do they know what good or adequate looks like?
Regulatory complexity and uncertainty	Perhaps more than other risks on the list, whilst there are common areas, there are a number of regulatory requirements that are sector specific. For HE, it's probably fair to say that there is a feeling that burden has increased – and we are entering a period of uncertainty as the Office for Students beds in. The report does ponder on the necessary resource to ensure compliance (whatever the sector) and, if possible, how the compliance requirements can be used to aid more strategic decision making.
Pace of innovation	An interesting area covered is the pace of innovation and how market leaders increasingly have to think like start-ups in order not only to defend their market decisions but to spearhead innovation. The report asserts that the primary emphasis is transforming companies of the old, analogue economy to agile digital players that exploit back office optimisation and automation and harness big data for competitive advantage. Perhaps more than the other risks listed, this will play out in different ways across the sectors and organisations, however, it can't be ignored in HE: • is enough being done on back office optimisation – could, for example, there be more joint services across institutions – payroll, for example? • is there room for more 'co-opetition', i.e. open innovation strategies that see organisations, and in some cases competitors, co-operate to their mutual benefit and to progress their industries? • big data – data has become crucial to understanding customer behaviour and companies are looking at ways they can harness data to predict future sales and precisely target marketing to achieve higher conversion rates. Has this progressed as it should within HE? The Department for Education's regulatory consultation highlights that the Office for Students will use data to determine where intervention may be needed. In addition, there can be a tendency not to ask *why* before *how* when considering data. Many big data projects do not have a tangible return on investment that can be determined up front.

Risk Theme	Comment
Political uncertainty: Brexit and other unknowns	The report covers Brexit – and asks how resilient are organisations and how able to respond to Brexit and geopolitical changes. Some HEIs have a specific Brexit risk in their register whilst others have factored real or potential related risks into the main register. As we gain more clarity and / or institutions model potential scenarios, there could be a role for internal audit in assisting with the risk management (including opportunities) exercises.
Vender risk and third-party assurance	Third party risk has returned to the fore. This is in part because organisations continue to seek cost efficiencies from outsourcing and are increasingly migrating their operations to Cloud hosted services. Organisations must understand how exposed they are to interruption caused by a third party supplier suffering a cyber-attack, losing its licence to operate, becoming insolvent or simply failing to meet increased demand. There must be a clear view about how the organisation would respond to such a situation and whether contingencies are in place to maintain business continuity. This includes assessing the business resilience of third parties themselves by reviewing and querying their own governance and controls. With growing emphasis on human rights, cyber security, strong bribery governance and high environmental standards and the potential reputational fallout from third party incidents manifesting – it means that due diligence of suppliers and contractors has never been more important – and should be considered as part of the internal audit programme.
The culture conundrum	Culture can be defined in several ways including – shared values, attitudes standards and beliefs that characterise members of an organisation and define its nature. In other sectors, it has come to the fore - e.g. banks that have presented themselves as responsible lenders while at the same time employing aggressive sales incentives and targets that have resulted in the mis-selling of products. We also know it's relevant to HE – the practices and approaches from international agents has come under scrutiny in the past, for example. More broadly, as the sector moves into a more competitive, market driven environment, there may a need for more focus – what does an institution stand for, what does it hope to achieve and who does it aim to attract – will there be increased tensions to 'sell' the institution beyond or at odds with these aspirations?

Risk Theme	Comment
Workforces: planning for the future	In our opinion, perhaps one of the most important areas contained within the report. Is there enough focus at Board level on, for example: • how to attract and retain younger talent with the necessary skills and create new roles to ensure the future success of the business as the world becomes more digital? • are institutions working to retain talent by offering diverse opportunities, creating both vertical and horizontal career paths? • with all organisations under constant and continual pressure to change products, services and even business models as each new technology or innovation emerges, are they agile in terms of their skills and projects? Those companies that access the necessary skills and more successfully match those skills to their needs will be more effective in adapting and changing. • rapid advances in artificial intelligence and robotics mean that many jobs that were once carried out by humans are, or soon will be, automated for the first time. • assurances surrounding management of HR risk and assurance that the organisation's workforce planning strategy is in line with its strategic vision.

For more information please contact:

Richard Young
Director
t: 0161 247 2959
e: ryoung@uniac.co.uk
www.uniac.co.uk